Glossario

Questo glossario comprende molti dei termini usati con riferimento al bitcoin. Si tratta di parole usate di frequente nel testo quindi si consiglia di memorizzarle per una rapida consultazione.

indirizzo

Un indirizzo bitcoin si presenta come segue: 1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV ovvero una stringa di lettere e numeri che comincia con il numero "1". Così come usiamo un indirizzo email per farci spedire una email, alla stessa maniera utilizziamo il nostro indirizzo bitcoin per farci spedire dei bitcoin.

bip

Proposte di miglioramento per il Bitcoin. Un'insieme di proposte che i membri della comunità bitcoin hanno presentato per migliorare i bitcoin. Ad esempio, BIP0021 è una proposta per migliorare lo schema dell'uniform resource identifier (URI).

bitcoin

Il nome dell'unità di valuta (la moneta), il network e il software.

blocco

Un gruppo di transazioni, marcate da un timestamp e dall'impronta univoca del blocco precedente. Per poter fornire una proof of work, è necessario calcolare l'header del blocco, e successivamente validare le transazioni. I blocchi validi sono inseriti all'interno della blockchain principale mediante il consenso della rete.

blockchain

Una lista di blocchi validati, ognuno che collega il precedente fino al blocco di origine (genesis block).

conferme

Quando una transazione viene inclusa in un blocco, ha una conferma. Non appena un altro blocco verrà validato nella stessa blockchain, la transazione avrà due conferme, e così via. Sei o più conferme sono considerate una prova sufficiente che la transazione non possa essere annullata.

difficoltà

Un'impostazione valida per tutta la rete, che regolamenta quanta potenza computazionale è necessaria per produrre una soluzione proof of work.

livello di difficoltà

La difficoltà a cui tutta la potenza computazionale della rete troverà nuovi blocchi approssimativamente ogni 10 minuti.

retargeting del livello di difficoltà

Un ricalcolo della difficoltà per tutta la rete, che si verifica ogni 2.016 blocchi, e tiene in considerazione la potenza di calcolo dei 2.016 blocchi precedenti.

commissioni

Il mittente di una transazione, spesso include il pagamento di una tariffa per la rete, che processerà la transazione richiesta. La maggior parte delle transazioni richiede il pagamento di una tariffa minima di 0.5 mBTC

hash

L'impronta digitale di un certo input binario.

genesis block

Il primo blocco della blockchain, utilizzato per inizializzare la criptovaluta.

miner

Un nodo della rete che trova soluzioni valide alla proof of work per i nuovi blocchi, mediante numerosi calcoli.

rete

Una rete peer-to-peer che propaga le transazioni e i blocchi a tutti i nodi bitcoin della stessa.

Proof-Of-Work

Una porzione di dati che richiede un significativo sforzo computazionale, per essere trovata. In bitcoin, i minatori devono trovare una soluzione numerica all'algoritmo SHA256 che soddisfa un obiettivo stabilito dall'intera rete, la difficoltà calcolata.

ricompensa

Un ammontare, incluso in ogni nuovo blocco, quale ricompensa dalla rete per il minatore che troverà la soluzione Proof-Of-Work. Al momento è pari a 25BTC per blocco.

chiave segreta (o chiave privata)

Un numero segreto che sblocca i bitcoin inviati all'indirizzo corrispondente. Una chiave segreta è rappresentata da una stringa alfanumerica simile a 5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh.

transazione

In parole povere, un trasferimento di bitcoin da un indirizzo ad un altro. Più precisamente, una transazione è una struttura di dati che esprime un trasferimento di valore. Le transazioni sono trasmesse attraverso la rete bitcoin, raggruppate dai minatori ed incluse all'interno di blocchi, registrati permanentemente nella blockchain.

wallet

Un software che conserva tutti i tuoi indirizzi bitcoin e le chiavi private. Usalo per inviare, ricevere e conservare i tuoi bitcoin.